4/

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,736	06/29/2001	Karanvir Grewal	P 0275038 P11033	3327

27496	7590	02/15/2005

PILLSBURY WINTHROP LLP
725 S. FIGUEROA STREET
SUITE 2800
LOS ANGELES, CA 90017

EXAMINER
ARANI, TAGHI T

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/893,736	GREWAL ET AL.
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>22 December 2004</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-16,19-23 and 25-28* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-16,19-23 and 25-28* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claims 1-16, 19-23, 25-28 are pending.

1.   The indicated allowability of claims 1-5, 6-16, 19-23, 25-28 is withdrawn in view of the

35 USC 112 issues raised with respect to independent claims 1, 6, 23 , 25 and 27 and newly

discovered reference(s) to D. Maughan et al., RFC 2409 . Rejections based on the newly cited

reference(s) follow.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

2.   Claims 1, 6, 23, 25 and 27 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

The term "more secure security configuration proposal is offered before less secure

security configuration proposal" in claim 1, 6, 23,25 and 27 is a relative term which renders the

claim indefinite. The term is not defined by the claim, the specification does not provide a

standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be

reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3.   Claims 1 3-7, 9-16, 19-23, 25-26 and 27 are rejected under 35 U.S.C. 103(a) as being

unpatentable over prior art of record, D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)",

Request for Comments (2409) and further in view of Maughan et al. (IDS filed 1/30/2003), "

Internet Security Association and Key Management Protocol (ISAKMP)", Request for

Comments (2408).

As per claims 1, 6, 23, 25 and 27, IKE (RFC 2409) discloses configuring a tunnel

comprising [RFC 2409 discloses processes for implementing negotiating virtual private network

(VPN) providing a remote user from a remote site access to a secure host or network see page 2,

2nd paragraph in Discussion]:

initiating, by a first peer, a negotiation with a second peer, the

negotiation including a plurality of security configuration proposals [Page 3, section 3.2,

SA or security association with one or more proposals which corresponds to plurality of

security configuration proposals provided by an initiator for negotiation, see page 9,

paragraph 6 wherein during security association negotiation, initiators present offers for

potential security associations to responders, see also page 23, section 7.1 phase 1 using

main mode];

sending, by the second peer, information to the first [page 24, in phase 1 using

main mode, the responders selects (i.e. extracts) , and returns one transform proposal];

extracting, by the first peer, a security configuration selected from among the

plurality of security configuration proposals from the information sent by the second

peer; and

establishing, using the security configuration, a tunnel between the first peer and

the second peer [page 5, in Phase 2 where security associations are negotiated on behalf

of service such as IPsec or any other service which needs key material and/or parameters

negotiation. RFC 2409 describes that "Quick Mode" accomplishes a phase 2 exchange.

RFC 2409 does not expressly disclose wherein the first peer orders the plurality of

security configuration proposals such that a more secure security configuration proposal is

offered before a less secure security configuration proposal.

However, Maughan et al. (RFC 2408) discloses that the first peer orders the plurality of

security configuration proposals such that a more secure security configuration proposal is

offered before a less secure security configuration proposal [page 19, paragraph 6, i.e. initiator

(i.e. first peer) sends a proposal containing more than one proposal which are sent in decreasing

preference which corresponds to ordering proposals such that a more secure security

configuration proposal (i.e. more preferred one) is offered before less secure security proposal

(i.e. less preferred one)].

It would have been obvious to one of ordinary skill in the art at the time the invention

was made to adapt the IKE protocol (RFC 2409) with the teachings ISAKMP (RFC 2408) to

have the first peer (i.e. initiator) to order the plurality of security configuration proposals such

that more secure security configuration proposal is offered before less secure security

configuration proposal to allow the second peer (responder) to make its policy take precedence

over the first peer (initiator) by selecting the proposal best suited for responder's local security

policy.

As per claims 3, 7 and 26, IKE (RFC 2409) discloses wherein the establishing a tunnel

includes conducting a phase2 negotiation in the IPSec protocol [page 5, in Phase 2 where

security associations are negotiated on behalf of service such as IPsec or any other service which

needs key material and/or parameters negotiation].

As per claims 4 and 5, IKE (RFC 2409) discloses initiating, by the first peer, a

preliminary negotiation with the second peer,

wherein the initiating a preliminary negotiation includes conducting a phase 1 negotiation

in the IPSec protocol [Phase 1 (or preliminary negotiation) where two ISAKMP peers establish a

secure, authenticated channel with which to communicate (i.e. a security association, SA). RFC

2409 discloses that " Main mode" and " Aggressive Mode" each accomplish a phase one

exchange].

As per claim 9, IKE (RFC 2409) discloses wherein the initiating comprises requesting,

by the first peer, that the second peer send information, the information including policy

information to define a subsequent negotiation between the first peer and the second peer [page

8, paragraph 6, i.e. Main mode is an instantiation of the ISAKMP Identity Protect Exchange].

As per claim 10, IKE (RFC 2409) discloses wherein the policy information defines one

or more security associations [page 5, section 3.4, a Security association is a set of policy and

keys used to protect information].

As per claim 11 and 15, IKE (RFC 2409) discloses wherein the information sent by

the second peer comprises sets of attributes, the attributes including security parameters and

network addresses [page 17, 4th and 6th paragraph, i.e. the identities of the SAs negotiated in

Quick Mode are implicitly assumed to be the IP addresses of the ISAKMP peers (**recited in**

claim 15), without any implied constraints on the protocol or port numbers allowed, unless client

identifiers are specified in Quick Mode and all offers made during a Quick Mode are logically

related and must be consistent. For example, if a KE payload is sent, the attribute describing the

Diffie-Hellman group (see section 6.1 and [Pip97]) MUST be included in every transform of

every proposal of every SA being negotiated. Similarly, if client identities are used, they MUST

apply to every SA in the negotiation].

As per claim 12 ,13 and 14, IKE (RFC 2409) discloses wherein the establishing a tunnel

comprises negotiating, by the first peer with the second peer, to generate a secure key,

wherein the negotiating to generate a secure key includes conducting a phase2

negotiation in the IPSec protocol [page 8, section 5 discloses that there are two basic methods

used to establish an authenticated key exchange: Main Mode and Aggressive Mode. Each

generates authenticated keying material from an ephemeral Diffie-Hellman exchange. Main

Mode MUST be implemented; Aggressive Mode SHOULD be implemented. In addition, Quick

Mode **(recited in claim 14)** MUST be implemented as a mechanism to generate fresh keying

material and negotiate non-ISAKMP security services].

As per claim 16, IKE (RFC 2409) discloses wherein a shared secret is stored on the

first peer before the negotiation [page 16, . 5.4 Phase 1 Authenticated With a Pre-Shared Key].

As per claims 19-22, IKE (RFC 2409) discloses wherein the negotiation utilizes the

base mode exchange extension of the IPSec protocol ,

wherein the initiating a negotiation further comprises sending, by the first peer to the

second peer, the identity of the first peer,

wherein the initiating a negotiation includes conducting a phase 1 negotiation in the

IPSec protocol,

wherein the negotiation utilizes one of main mode and aggressive mode of the IPSec

protocol [see page 16, section 5.4, Phase 1 Authenticated With a Pre-Shared Key for

limitations recited in claims 19, 20, 21 and 22 disclosing a key derived by some out-of-band

mechanism may also be used to authenticate the exchange. The actual establishment of this key

is out of the scope of this document.

When doing a pre-shared key authentication, Main Mode is defined as

follows:

```
       Initiator               Responder

       ----------              ----------

       HDR, SA          -->

                        <--  HDR, SA

       HDR, KE, Ni      -->

                        <--  HDR, KE, Nr

  HDR*, IDii, HASH_I  -->

                        <--  HDR*, IDir, HASH_R
```
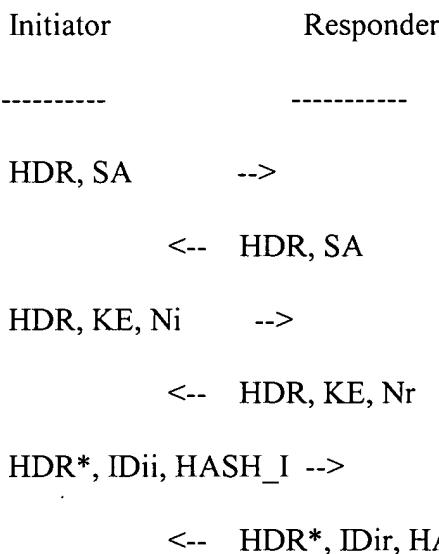
Aggressive mode with a pre-shared key is described as follows:

```
       Initiator               Responder

       ----------              ----------

  HDR, SA, KE, Ni, IDii -->

                        <--  HDR, SA, KE, Nr, IDir, HASH_R
```
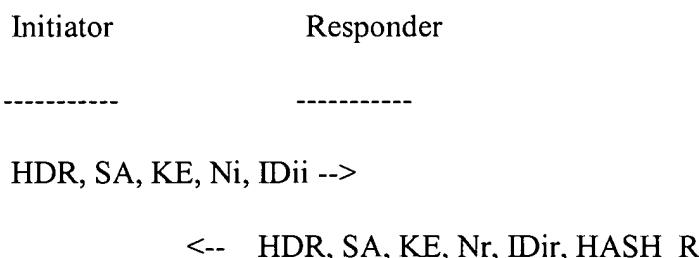
HDR, HASH_I   --

When using pre-shared key authentication with Main Mode the key can only be identified by the

IP address of the peers since HASH_I must be computed before the initiator has processed IDir.

Aggressive Mode allows for a wider range of identifiers of the pre-shared secret to be used. In

addition, Aggressive Mode allows two parties to maintain multiple, different pre-shared keys and

identify the correct one for a particular exchange].

4.   Claims 2, 8, 26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over

prior art of record, D. Harkins, D. Carrel as applied in claims 1, 6, 23, 25 and 27 above and D.

Dukes, R. Pereira, "ISAKMP Configuration Method", The Internet-Draft, March 2000 and

further in view of Y. Dayan, S. Bitan, "IKE Base Mode", Internet-Draft, January 2000.

As per claims 2 , 8, 26 and 28 The ISAKMP Configuration method (IDS#5) discloses a

new ISAKMP configuration method to allow IPsec-enabled entities to acquire and share

configuration information (i.e. negotiation comprises a request/reply negotiation), D. Dukes, R.

Pereira, page 11, section 7. That is, retrieving certain information from the other peer before the

non-ISAKMP SA can be established is sometimes useful, Y. Dayan, S. Bitan, page 3, section 1].

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The

examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).
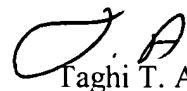
Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131
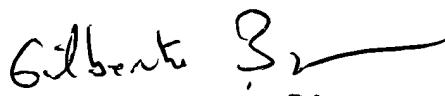
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100